Carnegie Mellon
Software Engineering Institute

Software Engineering Technical Practices

Survivable Systems Initiative

For more information, please contact—

SEI Customer Relations

Phone
412 / 268-5800

Email
customer-relations@sei.cmu.edu

World Wide Web
www.cert.org

Background

In 1988, as a result of an attack on the Internet, the SEI established the CERT® Coordination Center (CERT/CC), an emergency response team and a central point for communication among computer experts. Since then, the SEI has helped establish other response teams while maintaining leadership in analyzing vulnerabilities and threats. The SEI has extended its work to include survivable enterprise management and survivable network technology.

Goals

- Establish tools and techniques that enable typical users and administrators to effectively protect systems from damage caused by intruders.
- Establish techniques that help software engineers to model and predict security attributes of systems during development.

Benefits

The incident handling practices of the CERT Coordination Center have been adopted by more than 90 other incident response teams around the world. The time to resolve computer security incidents and repair computer system vulnerabilities has decreased significantly. Similarly, use of CERT security practices has improved resistance to attacks on networked computers and, thus, improved protection for the information stored on or transmitted by those computers.

Areas of Work

Survivable Enterprise Management

CERT Security Practices
CERT security practices provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices apply to many operating systems and platforms. Implementation details for specific operating systems accompany many of the practices.

Operationally Critical Threat, Asset, and Vulnerability Evaluation℠ (OCTAVE℠)
OCTAVE is a self-directed risk evaluation that allows an enterprise to identify the information assets that are important to the mission of the organization, the threats to those assets, and vulnerabilities that may expose the information assets to the identified threats. As a result, the enterprise can create a protection strategy that reduces the overall risk exposure of its information assets.

Curriculum Definition and Course Development
The Survivable Systems Initiative currently offers eight courses. Five courses derive from the work of the CERT Coordination Center, providing introductory and advanced training for technical staff and the management of computer security incident response teams. The initiative also offers three courses centered around broader Internet security issues and security practices. Its Information Security for Technical Staff is an intensive five-day course for system administrators and other technical staff members. Other offerings are geared toward educating policymakers, managers, and senior executives who are responsible for the security of information assets. Public courses are offered periodically and can be attended by any-

one, with a reduced charge for government personnel. In addition, customer-site courses are offered to individual organizations (a reduced fee is charged to government organizations).

Current course titles:

- Managing Computer Security Incident Response Teams (CSIRTs)
- Computer Security Incident Handling for Technical Staff (Intro)
- Computer Security Incident Handling Workshop for Technical Staff (Advanced)
- Overview of Managing a CSIRT
- Creating a Computer Security Incident Response Team
- Concepts and Trends in Information Security
- Information Security for Technical Staff
- Executive Role in Information Security: Risk and Survivability (by invitation only)

Survivable Network Technology

In the area of Survivable Network Technology, staff is concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems such as the Internet. Therefore, the technical approaches include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability tradeoff analysis, and the development of security architectures. This work draws on the CERT/CC's large collection of incident data.

Easel – an emergent algorithm simulation environment and language
Easel can be used to simulate the effects of cyber attacks, accidents, and failures, and can be used to predict the survivability attributes of complex systems while they are under development, preventing costly vulnerabilities before the system is built. Once completed, Easel will create dynamic depictions to help users envision global effects and enable "what-if" analysis as well as the study of cascade effects.

Survivable Network Analysis (SNA)
The SNA method provides a means for organizations to understand survivability in the context of their operating environments. The SNA method permits systematic assessment of the survivability properties of proposed systems, existing systems, and modifications to existing systems. The analysis is carried out at the architecture level as a cooperative project by a customer team and an SEI team.

Information Survivability Workshop
The annual Information Survivability Workshop is a forum for technologists developing methods and tools in various areas of information survivability. Lessons learned and case studies are shared. Participants strive for consensus on recommendations concerning specific problem areas and approaches, along with promising research directions and funding required.

CERT Coordination Center

Incident and Vulnerability Handling and Analysis
The SEI's CERT Coordination Center has become a major reporting center for incidents and vulnerabilities because the staff has an established

reputation for discretion and objectivity. As a result of the community's trust, the staff is able to obtain a broad view of incident and vulnerability trends and characteristics and to identify changing threats to Internet security. SEI staff communicates this information back to the community through reports, presentations at conferences and workshops, and training courses.

AirCERT
AirCERT is an open-source infrastructure being developed to automatically collect information on security events at Internet sites and automatically handle well-understood attacks. Components are currently being tested by the Internet community.

CERT Knowledgebase
The CERT Knowledgebase captures information related to network survivability and security. It provides data for analysis and a concrete basis for developing security improvement practices, evaluation techniques for security risk, and techniques for modeling and predicting security of systems while they are under development.

FedCIRC
The Federal Computer Incident Response Center (FedCIRC) was established to provide security services to federal civilian agencies. The CERT/CC performs security analysis for FedCIRC, which is managed by the General Services Administration.

Security Alerts
CERT advisories alert the Internet community to a current or imminent threat. Among the criteria for developing an advisory are the urgency of the problem, potential effect of intruder exploitations, and existence of a software patch or workaround. CERT summaries call attention to the types of attack currently being reported to the CERT/CC and provide pointers to advisories and other publications that explain how to deal with the attacks. Additionally, incident notes and vulnerability notes are informal means for providing timely information relating to security problems.

Computer Security Incident Response Team (CSIRT) Development
The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. It is essential to have multiple incident response organizations, each serving a particular user group. The CERT Coordination Center staff regularly works with sites to help their teams expand their capabilities and provides guidance to newly forming teams. In addition, courses for teams and their managers are available, as listed earlier.